나무위키

Tails OS

최근 수정 시각: 2026-08-16 00:48:26

분류:Debian | 2009년 출시 | 컴퓨터 보안 | 프라이버시

Linux 배포판

[펼치기 · 접기]

목차

1. 개요
2. 역사
3. 요구 제원
4. 뛰어난 파일 탐지 방어
   4.1. 파일 자체가 숨겨짐
   4.2. 파일 흔적이 숨겨짐
   4.3. 인터넷 이용 내역이 숨겨짐
   4.4. 뛰어난 급습 대처
5. Tails vs Whonix
6. 사용 방법 및 팁
7. 관련 문서

Tails OS 테일즈 OS	
개발사	The Tails project
출시일	2009년 6월 23일
최신 버전	7.10.1[1]
커널	Linux
라이선스	GNU GPLv3
한국어 지원	6.2버전부터 지원
홈페이지	

1. 개요

익명성 기능에 특화된 Debian 계열 Linux 운영체제.

에드워드 스노든이 NSA 기밀자료 폭로사건 당시 사용한 운영체제로 유명하다. 관련 한국 기사

2. 역사

- 2009년 6월 23일, amnesia 0.2가 출시됐다. Tails의 최초 이름은 amnesia(기억 상실증)였다. 지금도 사용자 계정 이름은 amnesia이다.
- 2009년 11월 27일, amnesia 0.3이 Mac을 지원하게 됐다. amnesia 0.3은 Mac을 지원하는 최초 버전이다.
- 2010년 4월 7일, 프로젝트 이름을 amnesia에서 The (Amnesic) Incognito Live System으로 바꾸었다. 이 이름은 2010년 5월 1일 발표된 버전 0.5부터 사용된다.
- 2011년 9월 21일, 버전 0.8이 발표됐다. 이 때부터 Tails라는 이름이 사용된다. 2012년 4월 27일, 버전 0.11 발표 글부터는 Tails라는 이름을 본문에도 포함한다.
- 2014년 4월 29일, Tails 1.0이 출시됐다. 향후 계획으로 Tails 1.1/2.0/3.0에 어떠한 기능이 들어갈지를 함께 서술하였다.
- 2014년 7월 22일, Tails 1.1이 출시됐다. 예고했던 대로 Debian 7 기반으로 바뀌었다.
- 2015년 9월 22일, Tails 1.6이 출시됐다. 1.6까지만 "The Amnesic Incognito Live System"이라는 이름을 사용한다.
- 2016년 1월 26일, Tails 2.0이 출시됐다. Debian 8 기반으로 바뀌었다.
- 2017년 2월 1일, Tails 3.0이 64-bit x86-64 아키텍처를 요구할 것이라고 밝혔다. 32-bit in86 아키텍처 사용자는 2016년 초 기준으로 약 4 %였고, 보안과 지속 가능성을 위해 레거시 지원을 중단하였다.
- 2017년 6월 13일, Tails 3.0이 출시됐다. Debian 9 기반으로 바뀌었고, 예고했던 대로 32-bit in86 아키텍처 지원을 중단하였다.
- 2019년 10월 22일, Tails 4.0이 출시됐다. Debian 10 기반으로 바뀌었다.
- 2022년 5월 3일, Tails 5.0이 출시됐다. Debian 11 기반으로 바뀌었다.
- 2022년 12월 20일, Tails 5.8이 출시됐다. 영구 스토리지를 만들거나 설정을 바꿔도 재부팅할 필요가 없도록 구조를 바꾸었다.
- 2024년 2월 27일, Tails 6.0이 출시됐다. Debian 12 기반으로 바뀌었다.
- 2024년 7월 15일, Tails 6.5가 출시됐다. Debian 12.6 기반으로 바뀌었다.
- 2024년 9월 26일, Tails와 Tor 프로젝트의 운영이 통합됐다.
- 2025년 9월 18일, Tails 7.0가 출시됐다. Debian 13 기반으로 바뀌었다.

3. 요구 제원

Tails 공식 홈페이지 요구 제원 및 권장 하드웨어 페이지

	권장 사양
프로세서	64비트 x86-64 아키텍쳐, IBM 호환[2]
RAM	3GB
용량 및 저장 공간	8GB 이상의 USB 또는 기록 가능한 DVD
추가 사항	외부 저장장치에서 부팅 가능할 것

4. 뛰어난 파일 탐지 방어

Tails는 파일 탐지를 방어하는 데 비용도 거의 들지 않고[3] 난이도도 일반인이 쉽게 따라할 수 있을 정도로 쉬우면서도 상당히 높은 수준의 보안이 달성된다. 가성비가 좋은 방어 방법이라고 말할 수 있다.

파일 탐지 방어를 위해 VeraCrypt와 같은 암호화 프로그램 하나만 달랑 쓰는 것은 전혀 안전하지 않다. 물론 트루크립트 암호화를 직접 깨는 것은 현재 기술로는 FBI, CIA, NSA, GCHQ가 와도 불가능하다.[4] 하지만 파일이 암호화되어 있다고 일이 다 해결되는 게 아니다. 운영 체제는 파일에 접근하기 위해 VeraCrypt 컨테이너를 마운트했을 때 그 안에 있는 파일들의 정보, 또는 VeraCrypt로 암호화하기 전에 가지고 있던 원본 파일에 관한 정보를 인덱싱할 수 있다.[5] 관련 보안뉴스 기사 캐시 데이터를 이용하면 VeraCrypt로 암호화한 파티션 내 데이터를 암호화된 파티션이 마운트되지 않은 상태에서도 알 수 있다.

ISP나 로컬 네트워크 관리자는 내가 인터넷으로 어떤 파일을 다운로드받았는지, 어떤 웹사이트에 접속하였는지가 담긴 로그를 보유하고 있으며, 이는 다운로드받은 파일을 내 컴퓨터에서 암호화시킨다고 해서 지워지지 않는다. 이런 상황에서는 파일 그 자체가 제아무리 단단하게 암호화돼 있다고 한들 아무 소용이 없다. 어쩌면 '보안이 유지되고 있다는 착각'(false sense of security)을 불러일으킬 위험마저도 있다. 파일 탐지 방어를 위해서는 Tails를 사용하는 것이 좋다.

파일을 탐지하려는 사람(이하 '공격자')은 파일을 은폐하려는 사람(이하 '방어자')의 취향을 크게 네 가지 경로를 통해 알아낼 수 있다.

1. 파일 자체를 찾아낸다.
2. 파일을 저장하였거나 실행한 흔적('최근 본 문서' 목록, 윈도우 탐색기에서 자동으로 생성되는 썸네일 등)을 찾아낸다.
3. 어떤 파일을 다운로드받았는지, 어떤 웹사이트에 접속하였는지 등 인터넷 이용 내역을 살펴본다.
4. 방어자가 파일을 작업 중일 때 갑작스레 문을 열고 들이닥친다.

Tails를 이용하면 이 네 가지 공격방법 모두에 대해 일정 수준 이상의 방어력을 갖출 수 있다.

4.1. 파일 자체가 숨겨짐

파일 자체를 찾아내려는 시도를 방어하는 것으로, 어떠한 파일의 내용을 가장 쉽고 확실하게 숨기는 방법은 암호화를 하는 것이다.

암호화는 단순히 운영체제 사용자 계정에 로그인 비밀번호를 설정[6]하는 것과는 전혀 다르다. 가령 "The Quick Brown Fox Jumps Over The Lazy Dog"이라는 내용의 텍스트 파일을 내부 저장장치에 저장해 놓고, 윈도우에 로그인 비밀번호를 설정해 두었다고 하자. 이 경우 내부 저장장치에는 "The Quick Brown Fox Jumps Over The Lazy Dog"라는 문장이 평문으로('그대로') 남아 있기 때문에 공격자는

1. 방어자의 컴퓨터 본체를 열고 내부 저장장치를 떼어가 공격자 자신의 컴퓨터에 연결하거나
2. Windows PE, Linux 라이브 부팅 등 운영체제 구성이 되어 있는 이동식 저장장치[7]로 부팅하여 저장장치 내부를 손쉽게 들여다 볼 수 있다.[8]

그러나 이 파일을 암호화시켜서 저장해 놓은 경우라면 다르다. 공격자가 내부 저장장치를 떼어가 자기 컴퓨터에 연결하더라도 공격자는 "e3ceqAHKc69Pk4gFMNbkRLQTqLJRMePnXzL6QJg"와 같은 암호화된 데이터만 보게 될 따름이다. 이 암호화된 데이터를 "The Quick Brown Fox Jumps Over The Lazy Dog"라는 평문(cleartext)으로 해석해 내기 위해서는 암호화에 사용된 암호화 키(encryption key)가 필요하다. 암호화 키란 곧 암호화를 할 때 암호화 프로그램에 입력하는 비밀번호를 말하는 것이라고 이해하면 된다.[9]

Tails를 이용하면, Tails가 설치된 저장장치 내에 만든 파티션은 LUKS(Linux Unified Key Setup)로 암호화된다. 저장장치 용량이 부족해 다른 저장장치를 추가로 이용하는 경우에도 Tails는 그 저장장치를 GUI를 통해 간편하게 LUKS로 암호화할 수 있는 옵션을 제공한다.

Tails는 암호화를 쉽게 사용할 수 있다. 구체적인 방법 설명은 아래로 미룬다.

4.2. 파일 흔적이 숨겨짐

파일을 저장하였거나 실행한 흔적을 찾아내려는 시도를 방어한다.

파일을 암호화된 상태로 저장해 놓는다고 문제가 다 해결되는 것은 아니다. 공격자는 암호화된 파일 자체는 들여다 볼 수 없겠지만 '최근 본 문서' 목록에서 파일 이름을 알아낼 수도 있고, 탐색기가 자동으로 생성한 썸네일도 볼 수 있고, 브라우징 히스토리도 볼 수 있고, 시스템이 파일 검색 속도를 올리기 위해 파일들을 인덱싱해놓은 자료도 볼 수 있다. 내가 본 파일들의 파일명과 썸네일, 그리고 내가 그 파일을 다운받기 위해 들어간 웹페이지의 URL, 그 웹페이지에 접속한 시간 따위가 공격자에게 고스란히 노출된다면, 그 파일의 구체적인 내용이 비밀로 남는다고 해 봐야 도대체 무슨 소용이겠는가?

흔히 '데이터보다 메타데이터가 더 중요하다'고 말하는 게 바로 이런 맥락에서다. 물론 이것도 케바케겠지만, 데이터 그 자체는 별 가치 없는 경우가 많다. 사실 파일명이 노출된 이상 그 파일의 '구체적인 내용'이 비밀로 남는다고 보기도 어렵다. 파일명을 아는 공격자는 인터넷에서 그 파일을 손쉽게 찾아 내용을 들여다볼 수 있을 것이기 때문.

여기에 대해서는 '썸네일이나 브라우징 히스토리도 어차피 OS 설치 파티션(쉽게 말해, C 드라이브)에 저장되는 거니까 파티션을 통째로 암호화해 버리면 해결되지 않나?'라는 의문이 제기될 수 있다. 그러나 파티션을 통째로 암호화한다고 해도 이러한 리스크는 회피하기 어렵다. Windows의 BitLocker, macOS의 FileVault, Linux의 LUKS 등 파티션 전체를 통째로 암호화하는(full-disk encryption) 기술들은 그 파티션이 마운트돼 있지 않은 상황에서만, 즉 C 드라이브를 기준으로 본다면 '컴퓨터 전원이 완전히 꺼져 있는 상황에서만' 보호기능을 제공한다. 직접 C 드라이브에 BitLocker 암호화를 걸어 보면 쉽게 알 수 있다. 컴퓨터가 완전히 꺼져 있는 상태에서는 BitLocker 비밀번호를 제대로 입력하지 못하면 하드에 저장된 내용을 볼 수 없지만, 일단 BitLocker 비밀번호를 제대로 한 번 입력하고 윈도우를 완전히 부팅하고 나면 그 후로는 C 드라이브에 있는 어떠한 파일이든 (따로 비밀번호를 입력하지 않아도) 그냥 바로 열리지 않는가? 이것이 파티션 전체 암호화의 맹점이다. 컴퓨터를 항상 꺼 놓고 살 것이 아닌 이상, OS 설치 파티션에 전체 암호화를 설정해 놓는 것은 근본적인 해결책이 되지 않는다. 게다가 각종 안티바이러스나 구글 크롬 등의 프로그램들은 주기적으로 C 드라이브에 있는 파일들을 스캔해서 자기네 회사 서버로 보내기도 한다.

이러한 문제는 Tails를 이용하면 간단히 해결된다. Tails는 별도 외부 저장장치(보통 USB 플래시 드라이브)에 설치되고 램(RAM)에서만 구동되기 때문에 하드에는 흔적을 남기지 않는다. 램은 휘발성 메모리이므로 모든 사용을 마치고 컴퓨터를 끄고 시간이 지나면 램에 저장된 데이터는 완전히 사라지며, 🔗Tails는 전원이 끊어진 직후 수 분간 램에 남는 데이터마저도 없애는 추가 보안 조치도 되어 있다.
지금 사용하는 빠른 컴퓨터를 그대로 활용할 수 있다는 이점도 있다. 가령 성인물 시청 전용 컴퓨터를 마련해서 그 컴퓨터에 디스크 전체 암호화를 걸어 놓고, 작업을 할 때에만 켜서 보는 방법을 생각해 보자. 이걸 하려면 일단 전용 컴퓨터를 마련해야 하므로 돈이 많이 든다. 크기가 크므로 숨기거나 휴대하기도 불편하다. 스틱 PC를 마련해서 필요할 때마다 TV에 꽂아 쓰는 방법보다도 낫다. 스틱 PC는 그 조그만 하우징 안에 탑재된 저성능 CPU를 이용하므로 속도가 느린 반면, Tails는 스틱 PC보다 더 빠른 CPU를 이용하므로 웹페이지 로딩속도도 빠르고 고화질 영상도 원활하게 재생된다.

4.3. 인터넷 이용 내역이 숨겨짐

인터넷 이용 내역 열람 시도를 방어한다.

SK브로드밴드, kt, LG U+, 세종텔레콤 같은 인터넷 회사(ISP)들은 이용자들이 자사의 인터넷망으로 몇 년 몇 월 며칠 몇 시 몇 분 몇 초에 어떤 사이트에 들어갔는지 상세하게 기록한다.

ISP뿐 아니라 인터넷에 접속하기 전에 거치는 각종 네트워크를 들여다 볼 수 있는 사람(가령 원룸에서 기본으로 제공하는 인터넷을 사용하는 경우 그 원룸 주인 및 같은 원룸에 사는 다른 세입자, 스타벅스 와이파이를 사용하는 경우 스타벅스 회사 및 같은 와이파이망에 접속해 있는 다른 손님, 집 공유기에 연결된 컴퓨터를 사용하는 경우 가족 구성원 중 그 공유기를 만질 줄 아는 사람 및 집 공유기 Wi-Fi에 비밀번호를 설정하지 않은 경우 그 네트워크에 접속해 있는 다른 사람)도 마음만 먹으면 아주 쉽게 이용자들의 인터넷 이용내역을 세세하게 기록할 수 있다.

한편, 웹사이트 운영회사들도 이용자들의 웹사이트 이용내역을 기록하는 것은 마찬가지다. 가령 구글에서 성인물 관련 단어를 검색하면, 내가 그날 그 시간에 구글에서 그 단어를 검색했다는 사실이 구글 서버에 기록으로 남는다. 만약 가족의 구글 아이디로 로그인된 상태에서 그렇게 했다면, 그 가족은 자신의 계정 내 '내 활동' 페이지에 들어가서 자신의 검색 기록을 조회하는 방법으로 그 사실을 손쉽게 알아 낼 수 있다.

인터넷 이용내역을 숨기는 도구로서 가장 흔히 쓰이는 것은 VPN이다. 그러나 VPN은 생각만큼 안전하지 않다. VPN은 ISP가 내 인터넷 이용내역을 들여다보는 것을 막아 줄 뿐이다. 웹사이트 운영회사가 내 인터넷 이용내역을 들여다보는 것은 제아무리 VPN을 쓰더라도 피할 수 없다. 가령 VPN을 통해 구글에 접속해 성인물 관련 단어를 검색하더라도, 구글은 Browser Fingerprinting(브라우저 정보 등을 이용하여 로그인 없이도 사용자를 특정하는 기술) '내가' VPN을 거쳐 자사의 웹사이트에 접속하여 성인물 관련 단어를 검색했다는 사실을 알게 된다. 게다가 Website Fingerprinting이라는 것이 있기 때문에 VPN을 쓴다고 꼭 ISP로부터 안전해지는 것도 아니다. 가령 어떤 차단된 페이지를 로딩할 때 브라우저가 특정한 패턴으로 패킷을 주고받는다는 사실이 알려져 있다고 하자. VPN을 쓰는 경우, ISP는 이용자가 자사 DNS 서버에 그 페이지의 도메인에 해당하는 IP 주소가 어디인지 물어본다는 사실도 알 수 없고, 이용자가 해당 페이지에 해당하는 IP 주소에 접속하고 있다는 사실도 알 수 없지만, 그 대신 이용자가 VPN 서버와 어떻게 패킷을 주고받고 있는지는 알 수 있다. 만약 이 패턴이 해당 페이지 접속 시 나타나는 패턴과 유사하다면, ISP는 '이 이용자가 VPN을 통해 그 페이지에 접속하였구나!'라고 추론할 수 있다.[10]

VPN보다는 Tor Browser를 이용하는 것이 낫다. Tor 브라우저는 Browser Fingerprinting 방어 능력이 갖추어져 있으므로, Tor 브라우저를 통해 검색을 하면 구글은 '어떤 익명의 Tor 이용자가' 그 검색을 했다는 사실은 알 수 있지만 '정확히 누가' 그 검색을 했는지는 쉽게 알 수 없다. 또한 Tor는 그동안 Website Fingerprinting에 대해서도 VPN보다는 나은 방어능력을 보여 왔고[11] 방어를 위한 기능이 계속 추가되는 중이기도 하다.

Tails를 사용하면 모든 네트워크 트래픽이 Tor를 거치도록 할 수 있다.

4.4. 뛰어난 급습 대처

Tails로 비밀스러운 작업을 하던 중 갑자기 공격자가 들이닥칠 경우, Tails 부트 미디어를 제거하면 곧바로 모니터가 까매지고, 잠시 기다리면 컴퓨터가 종료된다. 이는 공식적인 종료 방법이나 권장되지는 않는데, 영구 스토리지에서 읽기/쓰기 작업이 진행되는 도중에 제거할 경우 데이터가 깨질 수 있다. 이는 Windows에서 하드웨어 안전 제거를 하지 않고 제거할 때에도 발생할 수 있는 문제이다.

5. Tails vs Whonix

두 운영 체제는 개인정보 보호 면에서 양대산맥이라고 말할 수 있다.

Whonix는 IP 유출을 막는 데, Tails는 공격자 급습에 대비하는 데 강하다. Whonix는 이용하다가 악성코드를 먹어도 원래의 IP를 취득하기 힘들다. Tails는 누가 들이닥쳐도 설치된 저장장치를 제거하면 컴퓨터가 바로 꺼지고 컴퓨터로 뭘 했는지 알 수 없다.

Whonix는 가상 머신에서만 구동 가능하다. Tails는 가상 머신에서도 사용할 수 있지만, Native 사용을 권장한다. Whonix는 IP 추적 방지에, Tails는 컴퓨터 사용기록 인멸에 집중하였다. 자신에게 맞는 운영 체제를 사용하면 된다.

6. 사용 방법 및 팁

자세한 내용은 Tails OS/사용 방법 문서를 참고하십시오.

7. 관련 문서

- Tor
- 가상 사설망
- Whonix
- GrapheneOS

---

[1] 2026. 8. 15. 배포

[2] 32비트는 Tails 3.0부터 사용 불가하다.

[3] 이동식 저장장치(주로 USB 메모리) 구입비 5천 원 내외로 구축 가능하다.

[4] 사실 FBI나 CIA는 암호화 해독을 전문으로 하는 기관이 아니다. FBI는 우리나라로 치면 경찰청에 불과하고, CIA는 휴민트에 주력하는 첩보기관이다. 암호화 전문 기관은 아무래도 NSA.

[5] macOS는 터미널에서 qlmanage -r cache 명령어를 입력하여 캐시 데이터를 삭제할 수 있다.

[6] Windows 비밀번호를 생각하면 된다.

[7] Tails도 포함된다.

[8] 이러한 공격을 막으려면 튼튼한 케이스에 잠금장치를 설치하고 BIOS/UEFI에 암호를 설정하는 등의 작업을 하여야 한다. 이 작업을 해도 케이스를 강제로 깨면 내부 저장장치는 탈취당할 수 있으므로 안전한 방어가 아니다.

[9] 구체적으로는 비밀번호를 PBKDF2, scrypt 등 key derivation function에 통과시켜서 나온 해시값을 가지고 keystore에 저장된 master key candidates를 복호화한 다음, 복호화된 master key를 가지고 실제 데이터를 복호화하는 것. 하지만 유저 입장에서는 그냥 "비밀번호 = 암호화 키"라고 이해하면 충분하다.

[10] 그러니까 꼭 외국에 있는 VPN 서버 운영자의 협조가 있어야만 VPN 이용자를 추적(이른바 "역추적")할 수 있는 것은 아니다. 우리나라에 있는 ISP, IT 기업들도 얼마든지 VPN 이용자를 추적해 낼 수 있다.

[11] 관련 자료

이 문서의 내용 중 전체 또는 일부는 야한 동영상/좋은 은폐 방법 문서의 r98 판에서 가져왔습니다. 이전 역사 보러 가기

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.